Oracle® Retail Xstore Suite

Compliance Briefing
Release 17.0

April 2018

ORACLE
RETAIL

ORACLE

Oracle Retail Xstore Suite Compliance Briefing

Summary

Oracle Corporation (Oracle) engaged Coalfire Systems Inc. (Coalfire), as a respected Payment Card Industry (PCI) Payment Application – Qualified Security Assessor (PA-QSA) company, to conduct an independent technical assessment of the Oracle Retail Xstore Suite 17.0 application. Coalfire conducted assessment activities including technical testing, architectural assessment, and compliance assessment. The full white paper authored by Coalfire is available under NDA.

In this briefing, excerpts from that paper will describe that the Oracle Retail Xstore Suite 17.0 application is ineligible for Payment Application – Data Security Standard (PA-DSS) validation, but can be installed in a manner to support the continued PCI compliance of your cardholder data environment with the guidance provided by Oracle in its generally-available documentation.

PA-DSS Eligibility

Not all payment applications are eligible for PA-DSS validation. To be eligible an application must store, process or transmit cardholder data as part of authorization or settlement and be sold as an off the shelf product to merchants.

After meeting the basic criteria there are 13 eligibility questions that must be answered for the application including, is the application only offered as Software as a Service, does the application have access to clear text cardholder data, etc. For complete list of eligibility requirements see:
https://www.pcisecuritystandards.org/documents/which_applications_eligible_for_pa-dss_validation.pdf?agreement=true&time=1487271058394

While the Xstore 17.0 POS application facilitates authorization and settlement activities, it does not handle or have access to clear text cardholder data or sensitive authentication data. Xstore 17.0 also depends on other software in order to meet PA-DSS requirements but is not bundled with supporting software rendering the solution ineligible for PA-DSS validation. For these two reasons, Xstore 17.0 is ineligible for PA-DSS validation.

The fact that Xstore is ineligible for PA-DSS validation should not be viewed negatively. The changes that make the application no longer eligible are that the application no longer has access to cardholder data, which was a security enhancement to the application.

About Oracle Retail Xstore Suite 17.0

Oracle Retail Xstore Suite 17.0 is an Enterprise Point of Sale (POS) solution that relies on third-party PA-DSS applications and Pin Transaction Security (PTS) approved hardware pin pads for handling of cardholder data during the authorization and settlement processes, allowing Oracle Retail Xstore Point of Service to achieve an 'Out of Scope' status.

Oracle Retail Xstore Suite 17.0 has various built-in components and optional components that customers can choose from. Although there are various versions of Xstore applications available, particularly Xstore 17.0 is the one currently ineligible for PA-DSS validation. Oracle Retail Xstore Point of Service 17.0 consists of Xstore POS, Xstore Office, and EFTLink applications. Xstore POS includes Xenvironment and Xstore Mobile. Xstore

Office consists of Xcenter and Xadmin applications. Xstore POS, Xstore Office, and EFTLink are hosted within the cardholder data environment (CDE) and are covered as part of this assessment.

Assessment Scope

The scope of this assessment was to validate that neither unencrypted credit card data nor sensitive authentication data was stored or transmitted by Xstore 17.0. Only the PA-DSS validated application deployed on the pin pad terminal integrated with the Xstore application receives the necessary cardholder data for transmission to payment processors.

Encryption occurs via hardware immediately following the swipe, tap or manual entry into the Verifone card devices that are PTS 3.x or higher approved devices.

A third-party PA-DSS validated payment application provided by the specific payment processor performs the transmission of cardholder data to the respective payment gateway over a secure connection.

Merchant PCI Compliance Scope

There will always be certain controls for PCI compliance that must be independently assessed in any merchant's environment, and PCI compliance will always apply to a merchant if cardholder data is transmitted, processed, or stored anywhere in its physical environment. Cardholder data that is manually entered within the POS application or swiped at the pin-pad terminal is still within scope for PCI Data Security Standard (DSS) validation in a merchant environment. However, if Oracle Retail Xstore Suite 17.0 is properly integrated in the merchant environment, then this solution remains ineligible for PA-DSS validation requirements. Xstore 17.0 application does not have features of manual entry of card data and neither does it receive cardholder data at any time.

Oracle Corporation
World Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065
U.S.A.

Worldwide Inquiries:
Phone: +1.650.506.7000
Fax: +1.650.506.7200
oracle.com